UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

FAN MILLS, individually and on behalf of all others similarly situated, Plaintiff, v. SAKS.COM LLC, Defendant.	Case No. 1:23-cv-10638 (ER) Honorable Edgardo Ramos

PLAINTIFF'S OPPOSITION TO DEFENDANT'S
MOTION TO DISMISS FIRST AMENDED COMPLAINT

BURSOR & FISHER, P.A.
Yitzchak Kopel
Israel Rosenberg
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: ykopel@bursor.com
irosenberg @bursor.com

Attorneys for Plaintiff

TABLE OF CONTENTS

PAGE(S)

TABLE OF AUTHORITIES

PAGE(S)

CASES

STATUTES

RULES

OTHER AUTHORITIES

Plaintiff Fan Mills ("Plaintiff") respectfully submits this opposition to Defendant Saks.com LLC's ("Saks" or "Defendant") Motion to Dismiss Plaintiff's First Amended Complaint (the "Motion" or "MTD") (ECF No. 31).

INTRODUCTION

Plaintiff alleges that Defendant, in violation of A.R.S. §§ 44-1376-1376.05 (the "Arizona Statute" or "Statute"), invaded her privacy by unlawfully spying on how she interacts with marketing emails she receives from Saks including logging the time and place she read emails from Saks, through spy pixel tracking software placed without Plaintiff's consent. Saks and other retailers use spy pixels to track its recipients' reading habits. Saks exploits this data to build customer profiles so it can sell and market more products to them. Its recipients may be aware that they receive marketing emails, but they are not aware of, nor do they consent to, Saks's surreptitious means of tracking their sensitive reading behavior. The Arizona Statute is designed to prevent this invasion of privacy. Because Plaintiff has Article III standing to bring her claim in this Court and because Plaintiff properly alleges a violation of the Arizona Statute, the Court should deny Defendant's Motion.

FACTS

This case involves Saks tracking Plaintiff's email reading activity without her consent. Compl. ¶¶ 4, 10, 44. As part of its marketing practices, Defendant captures and logs sensitive information through spy pixels including the time and place subscribers open and read their messages, how long the subscribers read the email, subscribers' location, subscribers' email client type, subscribers' IP address, subscribers' device information and whether and to whom the email was forwarded to. *Id.* ¶¶ 4, 9, 55, 61. Defendant tracks this sensitive email reading information in order to "[m]ap individual shopper behavior with granular segmentation to drive personalized

campaigns." *Id.* ¶ 37. The use of spy pixels is a "grotesque invasion of privacy" according to industry advocates. *Id.* ¶ 31.

From sometime in 2017 to October 2023, Plaintiff received promotional emails from Saks. *Id.* ¶ 8. Plaintiff most recently opened an email from Saks in October 2023. *Id.* Little did Plaintiff know Defendant was tracking and recording her sensitive email data every time she opened an email from Saks. *Id.* ¶¶ 9-10, 58-59. Saks logged the time and place where Plaintiff opened her emails, how long she read the emails, her location, her email client type, her IP address, her device information, and whether and to whom she forwarded an email. *Id.* ¶¶ 9, 55-56. Defendant's invasive surveillance of Plaintiff's sensitive reading habits and clandestine collection of her confidential email records invaded her privacy and intruded upon her seclusion. *Id.* ¶¶ 5, 61. Plaintiff never consented to Defendant's tracking practices. *Id.* ¶¶ 4, 6, 10, 44, 59.

Plaintiff alleges this conduct violates the Arizona Statute, A.R.S. § 44-1376.01. *Id.* ¶¶ 1, 52-62. The Statute was enacted in response to the Hewlett-Packard ("HP") pretexting scandal. *Id.* ¶ 28. The HP pretexting scandal involved HP's board surreptitiously procuring the telephone and email records of newspaper reporters in an effort to catch leakers. *Id.* ¶¶ 15-27. Congress held a hearing and brought to light HP's invidious behavior. *Id.* ¶ 26. During the hearing, Congress uncovered how HP used spy tracking software to record when, where, and who opened the emails that were sent to the newspaper reporters. *Id.* The discovery shocked the Congressional committee. *Id.* One Congressman called email trackers "equivalent to going through the mail in my mailbox." *Id.* In response, Congress passed the Telephone Records Protection Act, 18 U.S.C. § 1039, and Arizona passed A.R.S. §§ 44-1376-1376.05. *Id.* ¶¶ 27-28.

ARGUMENT

I. PLAINTIFF HAS ARTICLE III STANDING TO BRING HER CLAIMS

Defendant argues that this Court lacks subject matter jurisdiction because Plaintiff's

allegations "fall far short of being particularized or concrete." MTD at 8. Defendant is wrong. Defendant's intrusions are "highly offensive," and courts in this district and elsewhere have repeatedly held that violations of statutes based on the torts of invasion of privacy or intrusion upon seclusion give rise to Article III standing.

A. Legal Standard

"Article III of the United States Constitution confines the judicial power of the federal courts to cases in which the plaintiff shows, *inter alia*, that she suffered a concrete injury in fact." *Metcalf v. TransPerfect Translations Int'l, Inc.*, 2023 WL 2674743, at *4 (S.D.N.Y. Mar. 29, 2023) (Ramos, J.) (citing *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021)). "The Second Circuit has described the injury-in-fact requirement as 'a low threshold.'" *Id.* (citing *John v. Whole Food Markets Grp., Inc.*, 858 F.3d 732, 736 (2d Cir. 2017)). "Because standing is challenged on the basis of the pleadings, we accept as true all material allegations of the complaint, and must construe the complaint in favor of the complaining party." *Bohnak v. Marsh & McLennan Companies, Inc.*, 79 F.4th 276, 283 (2d Cir. 2023) (quoting *W.R. Huff Asset Mgmt. Co., LLC v. Deloitte & Touche, LLP*, 549 F.3d 100, 106 (2d Cir. 2008)). "For standing purposes," the Court must "accept as valid the merits of [plaintiff's] legal claims. *Fed. Election Comm'n v. Cruz*, 596 U.S. 289, 298 (2022).

B. Defendant's Invasion Of Plaintiff's Privacy Is An Injury In Fact

Defendant argues that Plaintiff fails to allege "a concrete injury or … that the alleged harm caused by a read receipt bears a close relationship to harm suffered from intrusion upon seclusion. MTD at 9. Defendant is wrong. Plaintiff alleges concrete harm that constitutes an injury in fact under Article III.

1. Plaintiff Alleges a Concrete Harm

Defendant categorizes the invasion of privacy caused by its pixel pixels as being "benign." MTD at 8. That is wrong. The trackers used by Defendant "capture and log sensitive information

including the time and place subscribers open and read their messages, how long the subscribers read the email, subscribers' location, subscribers' email client type, subscribers' IP address, subscribers' device information and whether and to whom the email was forwarded to." Compl. ¶ 4. This amounts to an "invasive surveillance of Plaintiff's sensitive reading habits." *Id.* ¶ 5.

Lawmakers and industry experts have repeatedly recognized that the use of spy pixels is a privacy violation. Congressman Michael Burgess called it "equivalent to going through the mail in my mailbox." Compl. ¶ 26. Then-congressman Jay Inslee said "Speaking for the 600,000 people I represent, I think ***their expectations of privacy*** is that a corporation would not use tracer technology to try to follow where they send e-mail …. That's the ***expectation*** that my constituents have." *Hewlett-Packard's Pretexting Scandal: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 109th Cong. 754 (2006) (statement of Rep. Jay Inslee) (emphasis added). "Invisible pixels used to track email activity are now an 'endemic' issue ***that breaches our privacy*** … ." Charlie Osborne, *Tracker pixels in emails are now an 'endemic' privacy concern*, ZDNET (Feb. 17, 2021)[1] (emphasis added). Industry expert, David Heinemeier Hansson, called the use of spy pixels a "***grotesque invasion of privacy***." *Id.* (emphasis added). "The most dangerous threat that email tracking poses is to consumer privacy and personal safety." Mikael Berner, *The Business of Email Tracking: What To Know About Spy Pixels In Your Inbox*, FORBES (Jun 9, 2022).[2] Defendant may think that using spy pixels is

[1] https://www.zdnet.com/article/spy-pixels-in-emails-to-track-recipient-activity-are-now-an-endemic-privacy-concern/
[2] https://www.forbes.com/sites/forbestechcouncil/2022/06/09/the-business-of-email-tracking-what-to-know-about-spy-pixels-in-your-inbox/?sh=2084ee793fec

harmless. But consumers clearly disagree.

2. Courts Have Historically Held That Harm To One's Privacy Gives Rise To Article III Standing

A "concrete" harm is something with at least a "close relationship" to a harm "traditionally" recognized as providing a basis for a lawsuit in American courts—such as physical harm, monetary harm, or various intangible harms. *Id.* at 424-25 (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340-41, (2016)). "For example, harm to one's reputation ***and privacy*** are intangible injuries that have been recognized as concrete." *Neor v. Acacia Network, Inc.*, 2023 WL 6930000, at *5 (S.D.N.Y. Oct. 19, 2023) (Ramos, J.) (citing *TransUnion*, 594 U.S. at 424-26) (emphasis added). "In looking to whether a plaintiff's asserted harm has a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts, we do not require an exact duplicate." *TransUnion*, 594 U.S. at 433.

"Moreover, where a legislature has conferred a cause of action for violation of a statutory prohibition, the legislature's 'judgment is instructive and important' in discerning whether the plaintiff has suffered an intangible yet concrete harm." *Ives v. Bath & Body Works, LLC*, --- F.Supp.3d ---, 2024 WL 1677526, at *3 (D.N.H. Apr. 18, 2024) (quoting *Spokeo*, 578 U.S. at 341). "Courts must afford due respect to [a legislature's] decision to impose a statutory prohibition or obligation on a defendant, and to grant a plaintiff a cause of action to sue over the defendant's violation of that statutory prohibition or obligation." *TransUnion*, 594 U.S. at 425. Indeed, a "legislature may 'elevate to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law.'" *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 621 (7th Cir. 2020) (quoting *Spokeo*, 578 U.S. at 341, 136 S.Ct. 1540), *amended on denial of reh'g en banc*, 2020 WL 6534581 (7th Cir. 2020). Where a plaintiff plausibly alleges the deprivation of certain "procedural right[s] granted by statute ... [he] need not allege any additional harm beyond the one

[the legislature] has identified." *Spokeo*, 578 U.S. at 342 (emphasis omitted).

Here, the Arizona legislature sought to enact this statute in order to protect the privacy rights of its constituents. The procurement of "communication service records," which include "subscriber Arizona Statute elevates Arizona residents' substantive privacy rights by prohibiting information," toll bills or "access logs," "records of the path of an electronic communication between the point of origin and the point of delivery" and "nature of the communication service provided, such as … electronic mail." A.R.S. § 44-1376.01. The Statute was passed to protect Arizona residents against such invasions of privacy. *See* Compl. ¶¶ 27-28. Moreover, the prohibition against collecting communication service records is not "an ancillary requirement" of the law—but at the "heart" of the Statute. A.R.S. § 44-1376.01 ("A person shall not … knowingly procure … [a] communication service record … ."); *see Ives,* 2024 WL 1677526, at *5 (finding transfer of driver's license information to be at the "heart" of New Hampshire's privacy law thus sufficient for Article III standing). Therefore, under *TransUnion* Plaintiff has alleged sufficient harm rising to "concrete injury" and has Article III standing to bring her claim in this Court.

Based on this, courts have held that violations of similar substantive privacy statutes, even if they are insufficient for a common law causes of action, give rise to Article III standing in light of *TransUnion*. For example, courts have found alleged violations of the Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710, which prohibits the sharing of video rental records, to be sufficient to give rise for Article III standing. *Salazar v. Nat'l Basketball Ass'n*, 2023 WL 5016968, at *6 (S.D.N.Y. Aug. 7, 2023) (Rochlon, J.) (finding Article III standing for VPPA violations because it is similar to intrusion upon seclusion under the Restatement (Second) of Torts § 652B (1977); *Carter v. Scripps Networks, LLC*, 670 F. Supp. 3d 90, 95 (S.D.N.Y. Apr. 24, 2023) (Castel, J.) (same); *Alex v. NFL Enterprises LLC*, 2023 WL 6294260, at *3 (S.D.N.Y. Sept. 27,

2023) (Carter, J.) (same); *Martin v. Meredith Corp.*, 657 F.Supp.3d 277, 282–83 (S.D.N.Y. Feb. 17, 2023) (Cote, J.) (same). The same is true for alleged violations of the Telephone Consumer Protection Act ("TCPA"), 47 U.S.C. § 227 *et seq.*, which prohibits unsolicited marketing calls and faxes. *Urgent One Med. Care, PC v. Co-Options, Inc.*, 2022 WL 16755154, at *5 (E.D.N.Y. June 1, 2022), *report and recommendation adopted*, 2022 WL 4596754 (E.D.N.Y. Sept. 30, 2022) (finding allegations of TCPA violations to be a "concrete" privacy invasion in light of *TransUnion*); *Dickson v. Direct Energy, LP*, 69 F.4th 338, 344, 348 (6th Cir. 2023) (finding a "ringless voicemail" in violation of the TCPA "bears a close relationship to the kind of injury protected by the common law tort of intrusion upon seclusion," satisfying *Spokeo* and *TransUnion*); *Drazen v. Pinto*, 74 F.4th 1336, 1345 (11th Cir. 2023) ("[T]he harm associated with an unwanted text message shares a close relationship with the harm underlying the tort of intrusion upon seclusion. … For that reason, the harms are similar in kind, and the receipt of an unwanted text message causes a concrete injury."). Violations of Illinois' Biometric Information Privacy Act, 740 ILCS 14 (2008), which prohibits the collection of a person's biometric information without consent, also give rise to Article III standing. *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 619 (7th Cir. 2020), *as amended on denial of reh'g and reh'g en banc* (June 30, 2020); *see also Ives*, 2024 WL 1677526, at *4 n.3 ("While *Bryant* preceded the Supreme Court's opinion in *TransUnion*, the Seventh Circuit has held that *Bryant* remains good law post-*TransUnion*. *See Cothron v. White Castle Sys.*, Inc., 20 F.4th 1156, 1161 (7th Cir. 2021)."). Courts have also found standing in other violations of substantive statutory privacy violations. *Carter*, 670 F.Supp.3d at 95 ("[P]laintiffs identified a concrete harm under a state law analog to the VPPA by alleging that defendants 'violated Plaintiffs' ***statutorily conferred right to privacy in their reading habits***—an intangible harm presenting ample constitutional mooring for Article III purposes.'") (citing *Pratt*

v. KSE Sportsman Media, Inc., 586 F. Supp. 3d 666, 678 (E.D. Mich. 2022) (emphasis added)); *Ives*, 2024 WL 1677526, at *5 (finding that transfer of driver's license information in violation of state law is "concrete harm" because "[t]he mere fact that a person's information may be readily observable or a matter of public record does not mean that the unauthorized intrusion upon such information fails to establish a concrete injury.").

Similar privacy intrusions, such as intercepting and sorting mail, *Miller v. Brooks*, 123 N.C. App. 20, 26 (1996), and obtaining phone call records, *Lawlor v. N. Am. Corp. of Illinois*, 2012 IL 112530, ¶¶ 8, 33-35, have been recognized to be actionable under the Restatement. Thus the standing element of this case is no different than violations of the VPPA, TCPA, and BIPA: just as those substantive violations—although they may not be "sufficiently offensive" to satisfy common law threshold—give rise to Article III standing because they have "close relationship to harms recognized by American courts," violations of the Arizona Statute also give rise to Article III standing. *Drazen*, 74 F.4th at 1345; *TransUnion*, 594 U.S. at 424.

To support its assertion that Plaintiff must allege facts that clear an undefined bar of "highly offensive" privacy violations, Defendant points to several instances where courts found no concrete injury in Fair Debt Collection Practices Act ("FDCPA"), 15 U.S.C. § 1692 *et seq.*, cases. MTD at 9-10, 11 (citing *Six v. IQ Data Int'l Inc.*, 673 F. Supp. 3d 1040 (D. Ariz. May 18, 2023), *Ciccone v. Cavalry Portfolio Servs., LLC*, 2021 WL 5591725 (E.D.N.Y. Nov. 29, 2021), and *Sputz v. Alltran Fin.*, 2021 WL 5772033 (S.D.N.Y. Dec. 5, 2021). But this analogy fails. The FDCPA is not primarily designed to elevate privacy interests nor does it "bear[] a close resemblance to a violation of [plaintiff's] right to privacy." *Williams v. Portfolio Recovery Assocs.*, LLC, 2022 WL 256510, at *3 (E.D.N.Y. Jan. 27, 2022) (discussing *Sputz*). The FDCPA was "enacted to eliminate abusive debt collection practices" and any privacy protections afforded

by the statute are ancillary. *Six*, 673 F.Supp.3d at 1047 (internal quotations omitted). Therefore, any analogy to invasion of privacy is a poor fit. *See Carter*, 685 F.Supp.3d at 242 n.2 (explaining that FDCPA is missing "the historic analogue of the tort of intrusion upon seclusion" and distinguishing *Sputz*); *see also Spitz v. Caine & Weiner Co., Inc.*, 2024 WL 69089, at *4 (E.D.N.Y. Jan. 5, 2024) (rejecting attempts to analogize FDCPA to other common law torts). The Arizona Statute, on the other hand, is designed solely to elevate Arizona residents' privacy rights and thus a substantive violation of the statute gives rise to Article III standing.

Defendant cites *In re BPS Direct, LLC*, 2023 WL 8458245 (E.D. Pa. Dec. 5, 2023) ("*BPS*"), an out-of-circuit case regarding wiretapping statutes, in support of its argument. There, a court in Pennsylvania found that the intercepted information was not sufficiently private to give rise to Article III standing. *Id.* at *9 (citing *Cook v. GameStop, Inc.*, 2023 WL 5529772 (W.D. Pa. Aug. 28, 2023)). Notably, this reasoning has been criticized by other courts. For instance, in addressing *Cook*, the holding on which *BPS* relies, another Pennsylvania federal court noted that this reasoning runs afoul of the Supreme Court's teachings. "[*Cook*] found that, for Article III standing purposes, it would be appropriate at the pleading stage to determine whether the harm alleged would be sufficient to establish harm under the closely connected traditionally harmful cause of action." *Emmett v. Delta Air Lines, Inc.*, 2024 WL 2816502, at *14 (W.D. Pa. June 3, 2024). "***But the Court is instructed more directly by the Supreme Court***." *Id.* (stating that *TransUnion* requires only a "close relationship" not an "exact duplicate" to traditional harm) (emphasis added). "In fact, in *TransUnion*, the Supreme Court found that the plaintiff's claim of harm can qualify for Article III standing, even if harm would not be established under the standards of the traditional harm the plaintiff's cause of action was closely related to." *Id.* (noting that the defamation cause of action in *TransUnion* did not meet the common law standard); *Schnur v. JetBlue Airways Corp.*,

2024 WL 2816552, at *7 (W.D. Pa. June 3, 2024) (same).

Further, wiretapping statutes are different because they do not identify the threshold for what data interception is considered private for a violation. *See* 18 Pa.C.S. § 5703 (prohibiting the interception of "***any*** wire, electronic or oral communication") (emphasis added). In other words, these statutes do not "elevate" the privacy interest in of a certain data ***type***, the statutes just prohibit a ***manner*** of invasion—wiretapping. The court, therefore, was faced with a question: what is the minimum threshold considered private enough to give rise to Article III standing in a wiretap violation? Because the statutes are silent on this point, the court found that interception of "any" information is too low of a threshold. *Id.*, 2023 WL 8458245, at *10-12 (rejecting the argument that "the conduct of the wiretapping itself, regardless of the sensitivity of the content captured" gives rise to standing). Because the wiretapping statutes do not elevate any specific private data types, the courts had to look to common law analogues to establish what is reasonably private. *Id.*, 2023 WL 8458245, at *10 (citing *Cook v. GameStop, Inc.*, 2023 WL 5529772 (W.D. Pa. Aug. 28, 2023)). Here, on the other hand, where the Arizona legislature elevated the privacy interest of a discrete data type—email records—Plaintiff is only required to allege the invasion specified by the statute just like a plaintiff in a VPPA, TCPA, or BIPA claim. *See In re BPS*, 2023 WL 8458245, at *16 n.174 (acknowledging that substantive violations of the VPPA constitute "concrete harm").

Defendant also cites *Aponte v. Ne. Radiology, P.C.*, 2022 WL 1556043 (S.D.N.Y. May 16, 2022), *appeal dismissed*, 2022 WL 4125739 (2d Cir. Aug. 9, 2022). But that case supports Plaintiff. In a short opinion concerning a data breach, Judge Briccetti reaffirmed that "[i]ntrusion upon seclusion is one of the "traditionally recognized harms" that may comprise an injury-in-fact" and that, in another case, "defendant's unauthorized access and monitoring of plaintiffs' web-browsing activity comprised injury-in-fact." *Id.* at *5. The motion was dismissed on other grounds

because other unauthorized third parties—not the defendant—breached defendant's systems. *Id.* Likewise, in *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, another (out of circuit) data breach case brought only with a common law privacy claim, the court found that the information leaked was insufficiently private for the common law claim and for Article III. *See James v. Walt Disney Co.*, --- F.Supp.3d ---, 2023 WL 7392285, at *6 (N.D. Cal. Nov. 8, 2023) (distinguishing *I.C. v. Zynga*). This is very different that the instant case where the substantive violation lies in a statutorily "elevated" privacy interest.

In sum, since Plaintiff alleges, like other violations of substantive privacy statutes, that Defendant violates her substantive privacy rights under the Arizona law, which does not need to be an "exact duplicate" of common law standard and yet is still "highly offensive," Plaintiff has cleared the bar to have Article III standing to bring her action in this Court.

II. SAKS VIOLATES THE ARIZONA STATUTE

A. Legal Standard

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citing *Twombly*, 550 U.S. at 556). The plaintiff must allege sufficient facts to show "more than a sheer possibility that a defendant has acted unlawfully." *Id.* (citing *Twombly*, 550 U.S. at 556). However, this "flexible 'plausibility standard'" is not a heightened pleading standard, *In re Elevator Antitrust Litig.*, 502 F.3d 47, 50 n.3 (2d Cir. 2007) (quotation marks and citation omitted), and "a complaint ... does not need detailed factual allegations" to survive a motion to dismiss, *Twombly*, 550 U.S.

at 555.

The question on a motion to dismiss "is not whether a plaintiff will ultimately prevail but whether the claimant is entitled to offer evidence to support the claims." *Sikhs for Justice v. Nath*, 893 F. Supp. 2d 598, 615 (S.D.N.Y. 2012) (quoting *Villager Pond, Inc. v. Town of Darien*, 56 F.3d 375, 378 (2d Cir. 1995)). "[T]he purpose of Federal Rule of Civil Procedure 12(b)(6) is to test, in a streamlined fashion, the formal sufficiency of the plaintiff's statement of a claim for relief without resolving a contest regarding its substantive merits" or "weigh[ing] the evidence that might be offered to support it." *Halebian v. Berv*, 644 F.3d 122, 130 (2d Cir. 2011) (internal quotation marks and citations omitted). Accordingly, when ruling on a motion to dismiss pursuant to Rule 12(b)(6), the Court accepts all factual allegations in the complaint as true and draws all reasonable inferences in the plaintiff's favor. *Nielsen v. Rabin*, 746 F.3d 58, 62 (2d Cir. 2014); *see also Twombly*, 550 U.S. at 556 ("[A] well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of those facts is improbable ...."). "For purposes of this rule, the complaint is deemed to include any written instrument attached to it as an exhibit or any statements or documents incorporated in it by reference." *Chambers v. Time Warner, Inc.*, 282 F.3d 147, 152 (2d Cir. 2002) (internal quotation marks and citations omitted); *Mtume v. Sony Music Ent.*, 408 F. Supp. 3d 471, 474 (S.D.N.Y. 2019) (Ramos, J.).

B. Defendant Procures Class Members' Communication Service Records

Defendant argues that the records it procures "are not included in the definition of 'communication service record.'" MTD at 12. That is wrong. The Statute prohibits the knowing procurement of a "communication service record" of any Arizona resident "without the authorization of the customer." A.R.S. § 44-1376.01(A)(1). And the definition for "communication service record" is very broad:

"Communication service record" ***includes*** subscriber information, ***including***

> ***name***, billing or installation address, length of service, payment method, telephone number, ***electronic account identification*** and ***associated screen names***, toll bills or ***access logs***, ***records of the path of an electronic communication between the point of origin and the point of delivery*** and the nature of the communication service provided, such as caller identification, automatic number identification, voice mail, ***electronic mail***, paging or other service features.

A.R.S. § 44-1376(1) (emphasis added).

Read in the light most favorable to Plaintiff, Plaintiff properly alleges Defendant procures an "access log" of her email reading habits in order to procure Plaintiff's "individual shopper behavior" so it can "drive personalized campaigns." A.R.S. § 44-1376(1); Compl. ¶ 37. This would necessarily require Defendant to correlate Plaintiff's "behavior" with her "name" or "electronic account identification" or "associated screen name" that is traceable to her. Defendant also uses spy pixels to "track messages sent and check the behavior of recipients." *Id.* ¶ 39. This is used to create "'tracking logs' of recipient activity." *Id.* ¶ 40. By collecting the time and place each email was opened, how long the subscribers read the email, subscribers' location, subscribers' email client type, subscribers' IP address, subscribers' device information and whether and to whom the email was forwarded to, Defendant procures "access logs" of the time and place where the email was opened and other email activity. A.R.S. § 44-1376(1); Compl. ¶¶ 4, 55, 57, 58, 60.

The dictionary definition is dispositive here. "When faced with an unsettled interpretation of state law, we proceed by carefully predicting how the state's highest court would resolve the uncertainty or ambiguity. *Tantaros v. Fox News Network, LLC*, 12 F.4th 135, 142 (2d Cir. 2021) (cleaned up). In Arizona, "[a]bsent a statutory definition, courts generally give words their ordinary meaning and may look to dictionary definitions." *In re Drummond*, 543 P.3d 1022, 1025 (Ariz. 2024). "Access" means "to open or load (a computer file, an Internet site, etc.)" and "Log" means "to make a note or record of: enter details of or about in a log." *Access*, Merriam-Webster, https://www.merriam-webster.com/dictionary/access (last visited April 12, 2024); *Log*, Merriam-

Webster, https://www.merriam-webster.com/dictionary/log (last visited April 12, 2024). Defendant, thus, "logs" each time Plaintiff "accesses" her emails. *See* Compl. ¶ 49 ("[S]py pixel are designed to extract … time ***logs*** of email ***access*** … ."") (emphasis added). "Access log" is a computer science term used to describe a file "that records all events related to … user access to a resource on a computer." Arfan Sharif, *What Is An Access Log*, Crowdstrike (Dec. 21, 2022), https://www.crowdstrike.com/cybersecurity-101/observability/access-logs. An access log allows "software developers [and] operation engineers … to monitor how their application is performing, who is accessing it, and what's happening behind the scenes." *Id.* The information collected by an access log includes the date and time of client access, the client IP address or hostname, and username. *Id.* "An access log is a list of all requests for individual files—such as … embedded graphic images and other associated files that get transmitted—that people … have made from a website. … These server logs record the history of page requests made to the server and other pertinent information." Andrew Zola, *Access Log Definition*, TechTarget, https://www.techtarget.com/searchsecurity/definition/access-log (last updated January 2022). This is exactly the kind of information that is captured by email spy pixels in order to procure Plaintiff's "individual shopper behavior." Compl. ¶¶ 35-44.

Defendant also procures the "records of the path of an electronic communication between the point of origin and the point of delivery" by tracking whether an email was forwarded. *See* Compl. ¶ 55 ("Defendant's spy pixels are designed to extract … logs of email forwarding data."); *Id.* ¶ 4, 9, 61; *Hewlett-Packard's Pretexting Scandal: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 109th Cong. 754 (2006), ("I think [people's] expectations of privacy is that a corporation would not use tracer technology to try to

follow where they send e-mail.") (statement of Rep. Jay Inslee).

Next, Defendant argues that Plaintiff's allegations fall short of those arising from the HP scandal "wherein the bad actors sought to recover information beyond merely reading the email and clicking on links therein." MTD at 13. This argument is wrong and irrelevant. Defendant's spy pixels are essentially indistinguishable from those used in the HP scandal. *See* Compl. ¶ 34; *Hewlett-Packard's Pretexting Scandal: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 109th Cong. 146-47, 153-54, 383 (2006) (describing how the email spy tracking works). More importantly, they violate the plain and unambiguous words of the statute, which forms the basis for the Court's resolution of this motion.

Finally, Defendant argues that since the spy pixel records when the email is opened it is "after the delivery" and thus cannot be "the point of delivery." MTD at 13 (emphasis removed). This is also wrong. Just because Plaintiff opened the email after it was delivered does not mean it cannot ***also*** record the point of delivery. "Point" means the place of delivery and the Plaintiff alleges, and Defendant does not dispute, that the spy pixel records the recipients' location. *See Point*, Merriam-Webster https://www.merriam-webster.com/dictionary/point ("a narrowly localized place having a precisely indicated position: a particular place"); Compl. ¶¶ 4, 9, 30, 55, 61. "After" is a temporal adjective, while "point" is spatial. They do not conflict with one another.

C. Defendant's Use Of Spy Pixels Is Not Permitted By A.R.S. § 44-1376.02

Defendant argues that A.R.S. § 44-1376.02 exempts its conduct of spying on email recipients under the Arizona Statute. That section reads, in pertinent part: "This article does not prohibit … an entity that maintains communication service records from obtaining, using, disclosing or permitting access to any … communication service record … [a]s may be necessarily

incident to the rendition of the service." But this section has no applicability to this case.

First, Defendant is not an "entity that maintains communication service records" similar to a "public utility" or a "telephone company." *Id.* That would apply to an email provider, such as Gmail, Yahoo Mail, Outlook, or the like. According to Defendant's interpretation, any entity that procures communication service records would be considered to be an "entity that maintains communication service records." That is circular and renders the language of this section, which explicitly limits its applicability to certain entities, completely obsolete. "Such an interpretation would effectively gut the statutory exception. … [A court] may not construe a statute in a way that defeats its purpose." *Tanque Verde Unified Sch. Dist. No. 13 of Pima Cnty. v. Bernini*, 206 Ariz. 200, 206 (Ct. App. 2003), *as corrected* (Nov. 6, 2003).

Moreover, the spy pixels are not by any means "incident to the rendition of the service." Here, "the service" referred to, is obviously the maintenance of communication service. That is not what Defendant does. Defendant sells clothing. The section references information "incident to the rendition of *the* service" not "*a* service." (emphasis added). The word "the" here is clearly referencing the aforementioned service of maintenance of communication service. Nothing in this section permits wholesale violation of the statute merely because there is a business-related purpose for doing so. Defendant's reading of this section is absurd. If accepted, it would swallow the prohibitions of the statute whole. *See Nicaise v. Sundaram*, 245 Ariz. 566, 568, ¶ 11 (2019) ("A cardinal principle of statutory interpretation is to give meaning, if possible, to every word and provision so that no word or provision is rendered superfluous.").

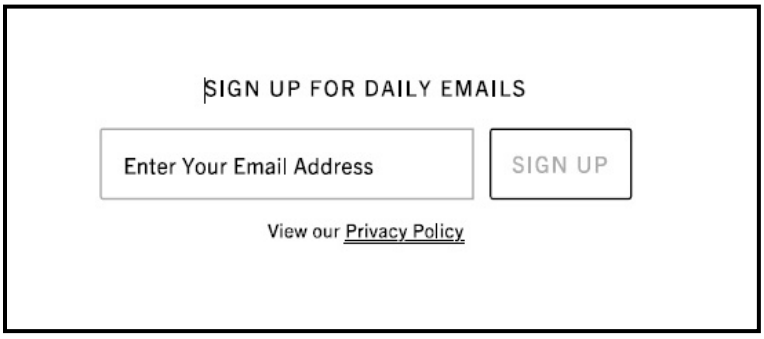
Moreover, even if Saks were a covered "entity" (which it is not), it is a factual question, not proper at the motion to dismiss stage, whether its spying is "necessarily incident" to the "rendition" of its marketing emails. Such determination is premature at this stage. *Roth v.*

Jennings, 489 F.3d 499, 509 (2d Cir. 2007) ("In any event, a ruling on a motion for dismissal pursuant to Rule 12(b)(6) is not an occasion for the court to make findings of fact.").

D. Plaintiff Did Not Authorize Defendant To Use Spy Pixels

Defendant argues that its procurement of communication service records was not "without authorization" because "when an individual accesses Saks's [sic] website or creates an online account … they agree to Sak's [sic] Privacy Policy." This argument is underdeveloped at this stage. *First*, Defendant is attempting to convert a Rule 12(b)(6) motion into a motion for summary judgement, which is improper at this stage. *See Friedl v. City of New York*, 210 F.3d 79, 83 (2d Cir. 2000) ("[A] district court errs when it considers affidavits and exhibits submitted by defendants … in a ruling on a 12(b)(6) motion to dismiss.") (cleaned up). Plaintiff alleges that she did not consent to Defendant's activities nor was she aware of it. Compl. ¶¶ 4, 6, 10, 28, 29, 44, 59. Defendant shows no testimony or evidence whether Plaintiff signed up online or elsewhere, whether Plaintiff consented to the Privacy Policy when she signed up, and whether the Privacy Policy at that time covered spy pixel tracking. Any such determination at this stage is premature. *Second*, even if Plaintiff signed up using the signup box shown in Defendant's Exhibit (a determination which is premature at this point), there is no "consent" or "I agree" to the Privacy Policy—just a "view our Privacy Policy" which is insufficient. *See Carter v. Ralph Laruen Corp.*, 2023 WL 4684559, at*8 (S.D.N.Y. July 20, 2023) (terms were not enforceable where the language surrounding the hyperlink "did not clearly signal to Plaintiff that, by continuing … she [would] be agreeing to the terms contained in [the] accompanying hyperlink.") (cleaned up); Ott Decl. Ex. B

at 5.



E. The Provisions Of Unrelated Laws Have Nothing To Do With This Case

Defendant makes two bizarre arguments that Plaintiff's allegation fails because it is (theoretically) insufficient to state claims under California wiretapping laws—unrelated laws. MTD at 15. That makes no sense. Plaintiff is not asserting a claim for violation of California's wiretapping laws and thus those courts have not "addressed this issue." *Tritschler v. Allstate Ins. Co.*, 213 Ariz. 505, 513 (Ct. App. 2006), *as corrected*, (Dec. 19, 2006).

For instance, Defendant argues that Plaintiff fails to allege that her information was intercepted "in transit." MTD at 15. That argument is based on Cal. Penal. Code § 631 which requires that information be intercepted "in transit." But the Arizona Statute contains no such requirement. Rather, it concerns procurement of private information, not wiretapping. As elaborated above, the Arizona Statute has nothing to do with wiretapping except that it is designed to protect privacy. Defendant's citation to the Statute's definition for "communication service record" similarly makes no sense. A communication service record is a record, not a wiretapping action.

Next, Defendant cites another case concerning California's wiretapping law finding that a website owner did not violate the statute because it "was the intended recipient of Plaintiff's communication" and "parties to a conversation cannot eavesdrop on their own conversation." *Williams v. What If Holdings, LLC*, 2022 WL 17869275 (N.D. Cal. Dec. 22, 2022). This argument

also makes no sense because the Arizona Statute has nothing to do with wiretapping. Here, the communication service record Defendant illegally procured was not a communication, it was a service record regarding a communication. Moreover, Plaintiff never intended to direct this information to Defendant, as was the case in *Williams*. Again, this silly argument would obviate the entire Arizona Statute if accepted.

F. The Legislative History Supports Plaintiff's Claim

Defendant argues that "Plaintiff's expansive reading of the Arizona Statute contradicts the Statute's legislative intent and legal history." MTD at 16-17. This argument is also unavailing. First, the Court must "predict" how an Arizona court would interpret the statute, *Tantaros*, 12 F.4th at 142, and in Arizona, courts do not rely on legislative history to derive legislative intent when the plain meaning of the statute is unambiguous, *State v. Ewer*, 254 Ariz. 326, 331 (2023) ("We do not consider legislative history when the correct legal interpretation can be determined from the plain statutory text."). As described above, the Arizona Statute is unambiguous.

Second, contrary to Defendant's assertion, the legislative history shows that the Arizona Statute was passed to prevent the kinds of invasions of privacy that occurred during the HP Pretexting Scandal which included email tracking with spy pixels. Compl. ¶¶ 14, 27; Arizona House Bill Summary, 2007 Reg. Sess. H.B. 2726 ("In January 2007, Congress passed the Telephone Records and Privacy Protection Act …. [the Arizona statute] prohibits a person from knowingly procuring … a communication service record."); *Hewlett-Packard's Pretexting Scandal: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 109th Cong. 16 (2006) (statement of Rep. Blackburn discussing the proposed Consumer Telephone Records Protection Act). Third, as Defendant noted, the statute was specifically amended—a year after it was originally passed—to include "communication service records," indicating that the statute is ***not*** limited to telephone pretexting. MTD at 16-17;

Arizona House Bill Summary, 2007 Reg. Sess. H.B. 2726; *see State v. Garza Rodriguez*, 164 Ariz. 107, 111 (1990) ("[W]e presume that by amending a statute, the legislature intends to change the existing law.").

Put simply, the plain language of the Arizona Statute prohibits the surreptitious collection of email records which includes logging the time and place where specific emails were read by Plaintiff. Defendant violated the Statute by tracking through a spy pixel Plaintiff's sensitive email reading habits including the time and place where she read her emails.

CONCLUSION

Plaintiff has properly alleged Defendant violates the Arizona Statute, A.R.S. § 44-1376.01, by tracking her email activity, and this Court has subject matter jurisdiction to hear this claim given that Plaintiff has Article III standing for her claim. For all the foregoing reasons, the Court should deny Defendant's Motion to Dismiss in full. To the extent the Court grants any aspect of Defendant's Motion, Plaintiff requests leave to amend. *See Conflict Int'l, Inc. v. Komorek*, 2024 WL 1347577, at *18 (S.D.N.Y. Mar. 29, 2024) (Ramos, J.) (granting leave to amend).

Dated: June 28, 2024

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Yitzchak Kopel*
Yitzchak Kopel

Yitzchak Kopel
Israel Rosenberg
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: ykopel@bursor.com
irosenberg@bursor.com

Attorneys for Plaintiff